16th Annual Security Technology Symposium and Exhibition

NDIA

June 26-29, 2000
Williamsburg, VA

Infrastructure Interdependencies: The Long Pole in the Tent

It's the end of the world as we know it: Security Interdependency in a Converged Networking Environment

Henry (Hank) M. Kluepfel CPP
973.543.7064
Henry.m.kluepfel@saic.com

SAIC’s Security Experience

SAIC

An Employee-Owned Company

- 20+ Years Protecting the ***Long Pole in the Tent*** for the U.S. Government and Fortune 500
- I&C e.g., Telecom, Energy, Transportation, Healthcare and Financial Customers in every major market and critical infrastructure segment

Unique Perspective of the Real Problem

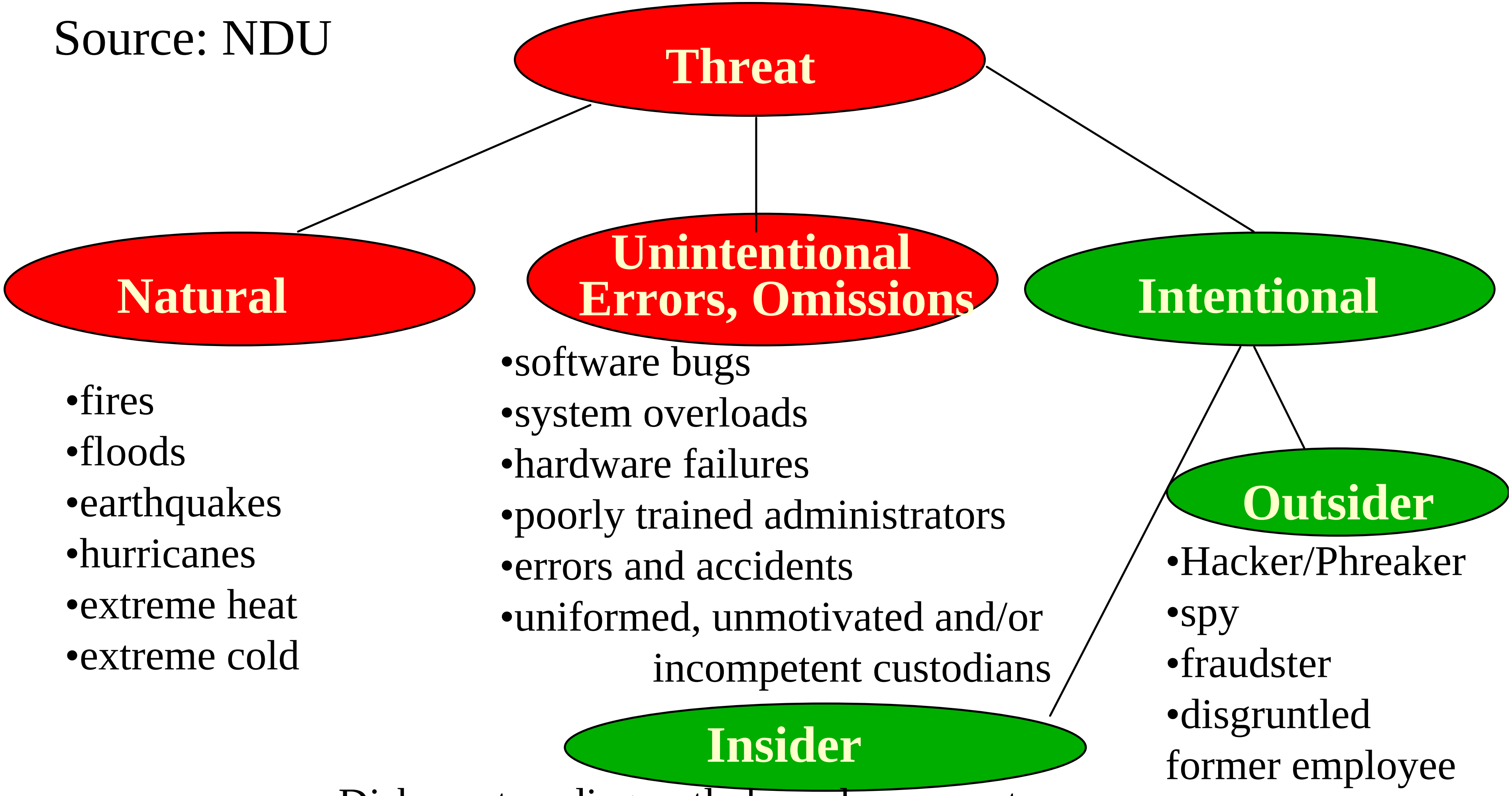
- Established first information exchanges on cyber & physical incidents, threats and vulnerabilities for telecom infrastructure
- *Consequence management requirements, simulation and modeling based upon real threats, growing interdependence and complexity*

CYBER TIMES EXTRA

www.saic.com
www.globalintegrity.com
www.telcordia.com

Traditional Threat Tree

Source: NDU



Threat

Natural

- fires
- floods
- earthquakes
- hurricanes
- extreme heat
- extreme cold

Unintentional Errors, Omissions

- software bugs
- system overloads
- hardware failures
- poorly trained administrators
- errors and accidents
- uniformed, unmotivated and/or incompetent custodians

Intentional

Outsider

- Hacker/Phreaker
- spy
- fraudster
- disgruntled former employee

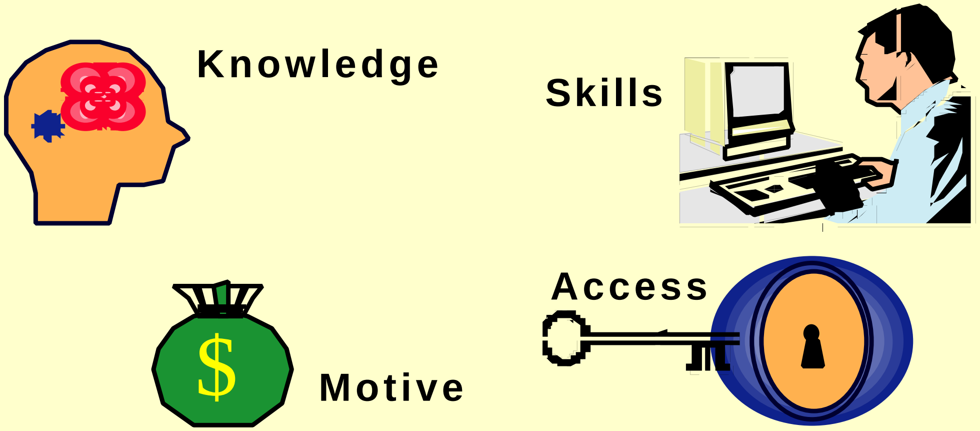
Insider

- Dishonest or disgruntled employee, partner, outsource employee or contract employee

Infrastructure Insecurity

Risk

- Exploitable Computer System or Network Vulnerabilities
- Lack of Loss Prevention, Detection, and Recovery Controls
- An Employee, Former Employee, Contract Employee, or an Outsider with the Skills, Knowledge, Access, and/or Motive (SKAM):



Risk is directly proportional to a computer's network seamless connectivity, implied trust and inherent vulnerabilities

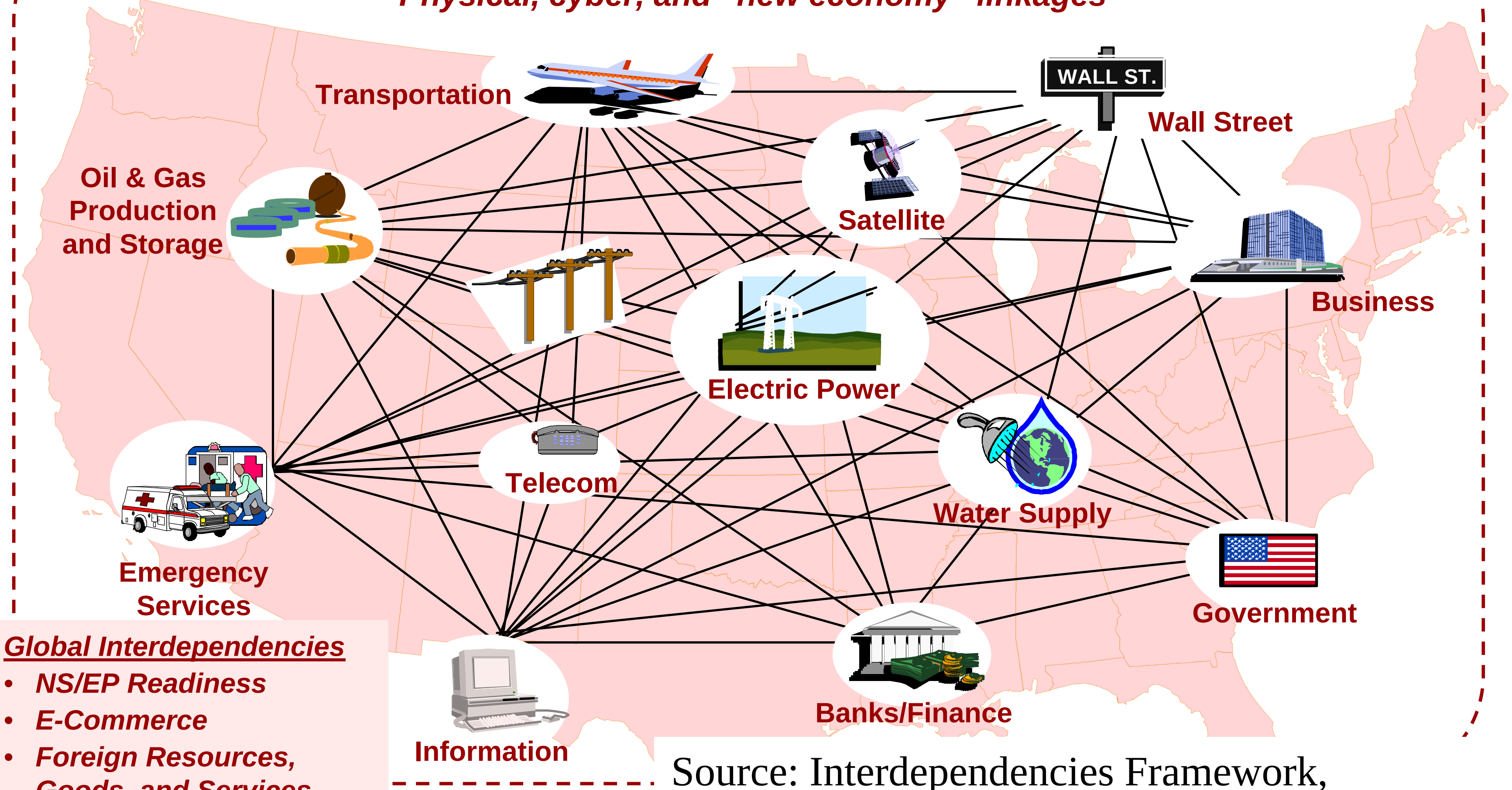
Cybercrime,Cyberterrorism & Cyberwarfare: Averting an Electronic Waterloo (CSIS'98)

The United States is now exposed to a host of new threats to the economy, indeed to the whole of society. It has erected immensely complex information systems on insecure foundations. The ability to network has far outpaced the ability to protect networks. ..In today's electronic environment, many haters can become a Saddam Hussein and take on the world's most technologically vulnerable nation. ...There is no shortage of terrorist recipes on the Internet, step-by-step cookbooks for hackers and crackers (criminal hackers) and cyberterrorists.

Our Critical National Infrastructures Are Mutually Dependent and Interconnected

An Employee-Owned Company

Physical, cyber, and "new economy" linkages



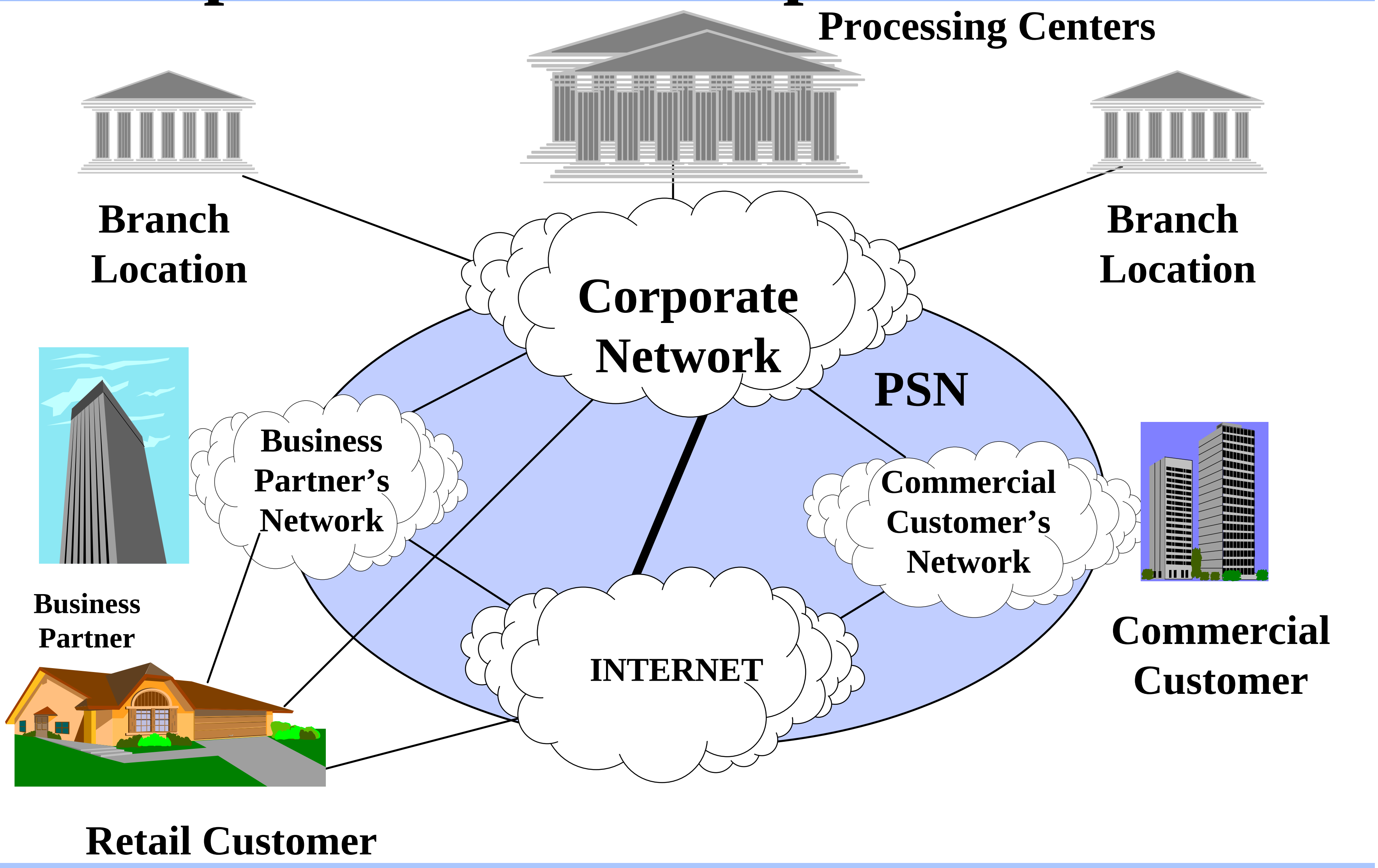
Global Interdependencies

- *NS/EP Readiness*
- *E-Commerce*
- *Foreign Resources, Goods, and Services*
- *Telecommunications*
- *...*

Source: Interdependencies Framework,
J. Peerenboom, Argonne National Lab

Critical Infrastructure Interdependencies: Example

An Employee-Owned Company



Critical Infrastructure Risk Assessments

"The NSTAC continues to serve as the premier example of industry offering its collective resources to assist the Government in addressing issues critical to the national interest."

- President Clinton, June 8, 1998

Assessment	Date
• Telecommunications	June '99
• Electric Power	Dec. '97
• Financial Services	Dec. '97
• Transportation	June '99

Most reports can be found at:

http://www.ncs.gov/nstac/NSTACReports.html

NSTAC on Network Convergence, May 2000

An Employee-Owned Company

"The convergence report is a good example of the excellent work done by the NSTAC Members…"

Dick Clarke, Special Assistant to the President and National Security Coordinator for Security, Infrastructure Protection and Counter-Terrorism, June 5, 2000

Executive Summary

- NS/EP community depends heavily on priority treatment of PN calls
- Public network architecture and technology platforms will change
- Potential implications for Government Emergency Telecommunications Services include new blocking sources, lack of ubiquity and interoperability, lack of access to GETS features, disparate congestion handling, and a lack of commensurate network reliability and security.
- NS/EP requirements are unlikely to be incorporated by industry unless the features needed to meet these requirements are standardized by industry
- The current level of security safeguards into GETS is inadequate
- As the Next Generation Network (NGN) evolves, telecommunications carriers' SS7 networks will become less discrete and more reliant on IP technology and interfaces. Therefore, it is necessary to consider the security, reliability, and availability of the NGN control space as it relates to the provision and maintenance of NS/EP service capabilities.

Camping tips: 5 places not to pitch a tent

Translation: NOT Build your business

http://allsands.com/Travel/HowTo/campingtipsca_rve_gn.htm

An Employee-Owned Company

- *A rabbit's home is his castle (re: Bugs Bunny Vs Highway Department,1957)*
  - Translation: The Internet: A Hacker’s home is his/her castle
- Bee's nests- not just for trees anymore
  - Translation: With hackers on the payroll- not just outsiders anymore
- Worker ants of the world, unite.
  - Translation: Hactivists, PHA Ankle biters of the world unite
- Lightning is a cruel mistress.
  - Translation: Interdependent with a vulnerable PN node
- They are called 'lowlands' for a reason
  - Translation: Avoid the low hanging fruit of non-compliant technology, personnel and markets

Network Interoperability: The Key to Competition

NRIC's Top Security Concerns

An Employee-Owned Company

- **Increased number of access points and networking**
- **Collocation of carriers into one carrier's infrastructure basket(s)**
- **Increased number of interconnected inexperienced systems administrators and processes**
- **Embedded Operations Channels of Signaling and Transport Protocols (e.g., SONET DCC, ATM OAM Cells, SS7 Network Management Messages) gives virtually unlimited access to everything and everyone connected (networked) to them**
- **Internet and Intranet Exploitable technology used for access to Network Operations and Signaling Systems**
- **Added complexity, dependencies and single points of failure**
- **Lack of Fidelity Bonds, Criminal Background Checks on insiders**
- **CALEA Control Requirements of Section 229 of the Act**

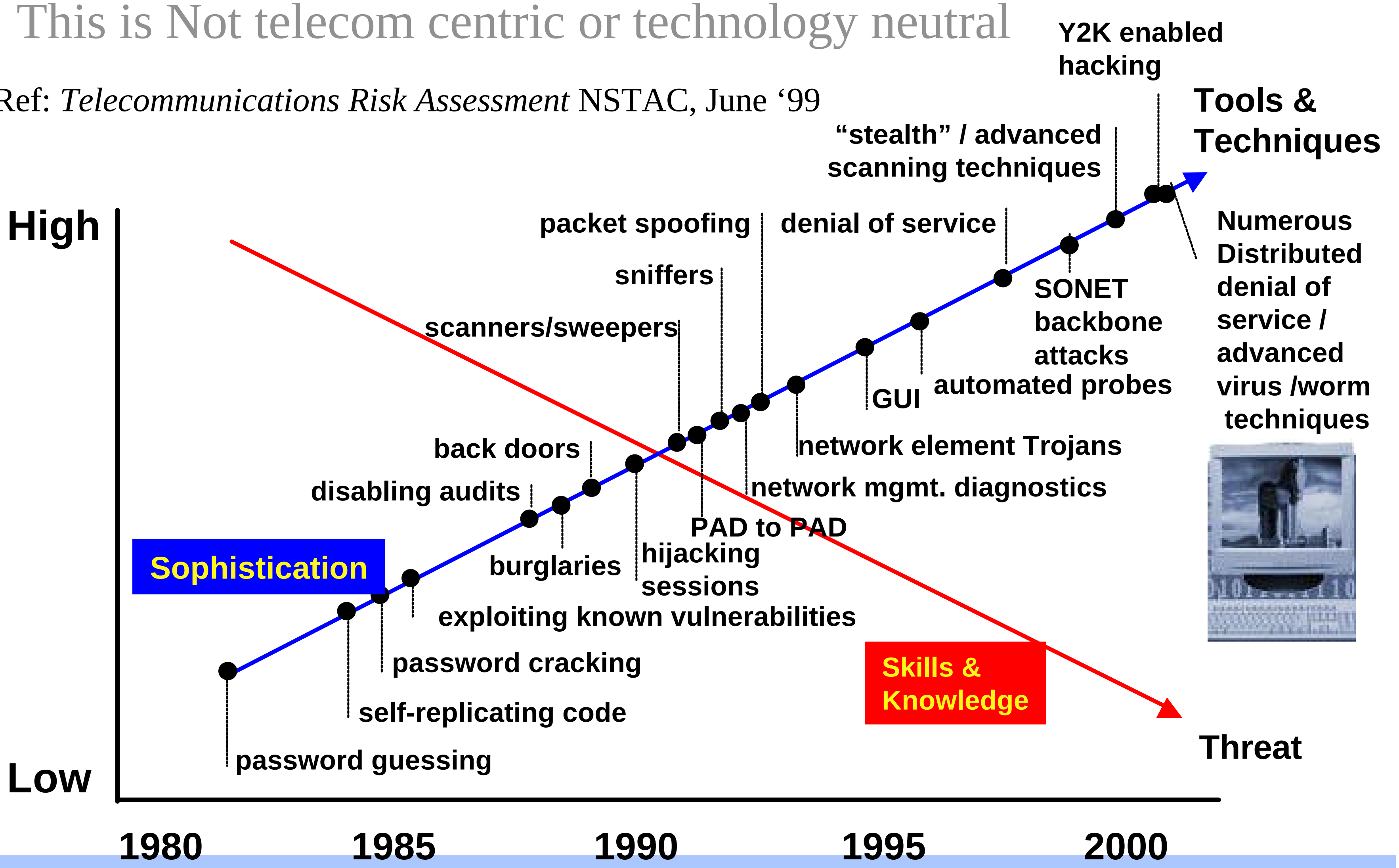
Source: NRIC 3 FG1 Operations Task Group www.nric.org

Decreasing Barriers Vs. Increased Sophistication:

An Employee-Owned Company

Note: This is Not telecom centric or technology neutral

Ref: *Telecommunications Risk Assessment* NSTAC, June ‘99



Telecom Incident's At A Glance:

An Employee-Owned Company

- High Tech Telecom Hacks Linked to Organized Crime
- High Tech Theft Strong Arm Burglaries of Central Offices
- Burglary of Central Offices and Centers
- Sophisticated Theft of Services
- Unindicted Co-Conspirators Often On Payroll with Privileges
- Theft of Intellectual Property & Privacy
- Sophisticated Fraud through network manipulation
- Law Enforcement Operations Targeted
- Y2K Enabled Hacking
- Vulnerable Operations: If its isn't in the release and administration neutral, its not patched or managed
- Virtually every case found by accident or error (clumsy hacks)

"Most Crimes Committed by the New Insiders"

Security Incident Root Causes:
A Baker's Dozen

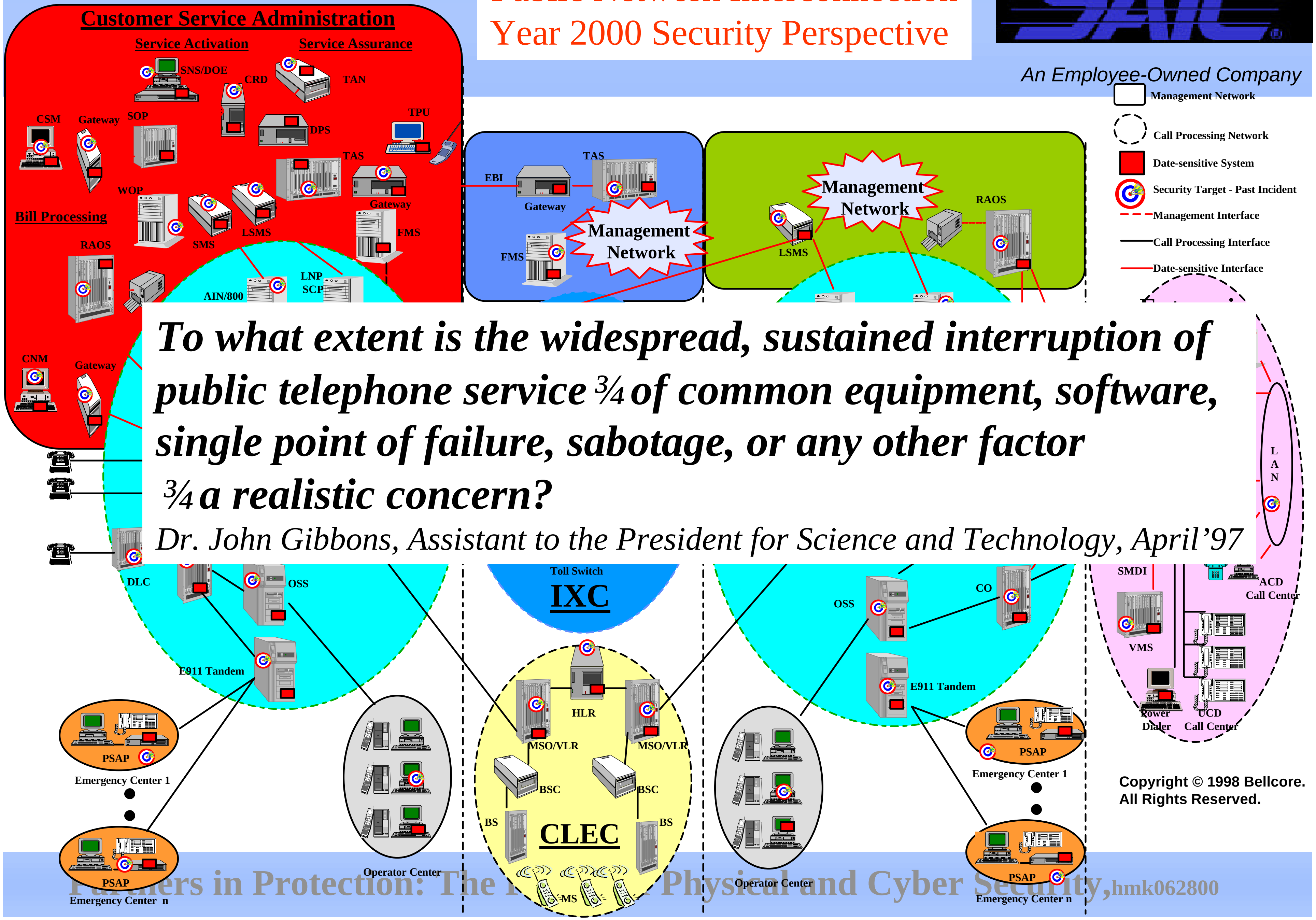
An Employee-Owned Company

- **Policy:**
  - Reactionary security architectures and firewalls
  - Not supported by administrators, users, and partners
  - Not reflected in contracts, procurements or practices
  - Not integrated w/ business planning **or acquisitions**
- **Behavior:**
  - Passwords were easy to guess or easy to compromise
  - Lack of awareness, training and certification on security
  - Re-engineering insecurity into killer applications
  - Code of Conduct not briefed, updated or enforced
  - Inadequate personnel screening & exit procedures
- **Technology:**
  - Powerful Diagnostic Tools with little or no access controls
  - Insecure defaults in most systems and networks
  - Holes in firewalls and Perimeter Buffer Zones (DMZs)
  - Complexity of systems failures tend to mask problem
  - Release 1 through 4 of COTS products full of holes

Public Network Interconnection
Year 2000 Security Perspective

SAIC®

An Employee-Owned Company



To what extent is the widespread, sustained interruption of public telephone service ¾ of common equipment, software, single point of failure, sabotage, or any other factor ¾ a realistic concern?

Dr. John Gibbons, Assistant to the President for Science and Technology, April'97

Risk Assessments by Pessimists (Optimists w/experience)

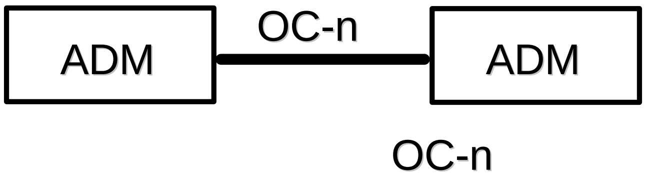
An Employee-Owned Company

Based on the success with which hackers and other (admittedly small-time) intruders have invaded or subverted parts of the network, it is not unreasonable to expect that a malicious assault upon the PSN by a serious team of aggressors attacking multiple targets has a realistic chance of forcing an outage of large scale and broad geographic range. The expertise required to pull off such an attack is not extreme, and is in fact within the capabilities of many technically competent, computer-literate people around the world. Because the service providers have no experience with this kind of forced outage, they may be unprepared to recover from it as promptly and successfully as they recover from natural disasters or equipment failures.

Next Generation Network Compromise: Fact or Fiction?

Bad things happen to Good Networks in the absence of Best Practices

- Reuse of previously exploited Default accounts & passwords
- Data Communications Channel had no screening
- Password aging features not supported
- Inconsistent and ambiguous documentation
- Data confidentiality not addressed
- Dial-up Modem pre configured for remote access
- Inadequate Access Control to Privileged Commands

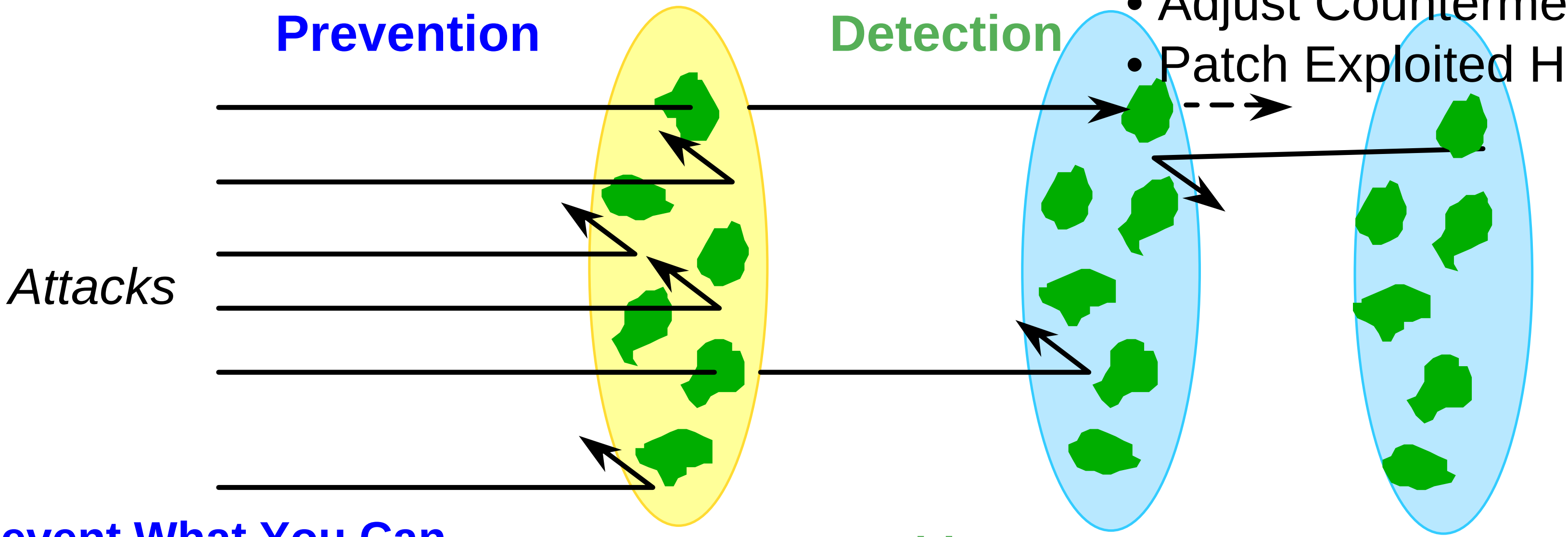


All you need in a low tech threat

Key to a Happy Camper: Meshing Prevention, Detection and Containment

An Employee-Owned Company

Source: Lunt, SecureComm98 Keynote



Recovery

- Restore Trust
- Adjust Countermeasures
- Patch Exploited Holes

Prevent What You Can

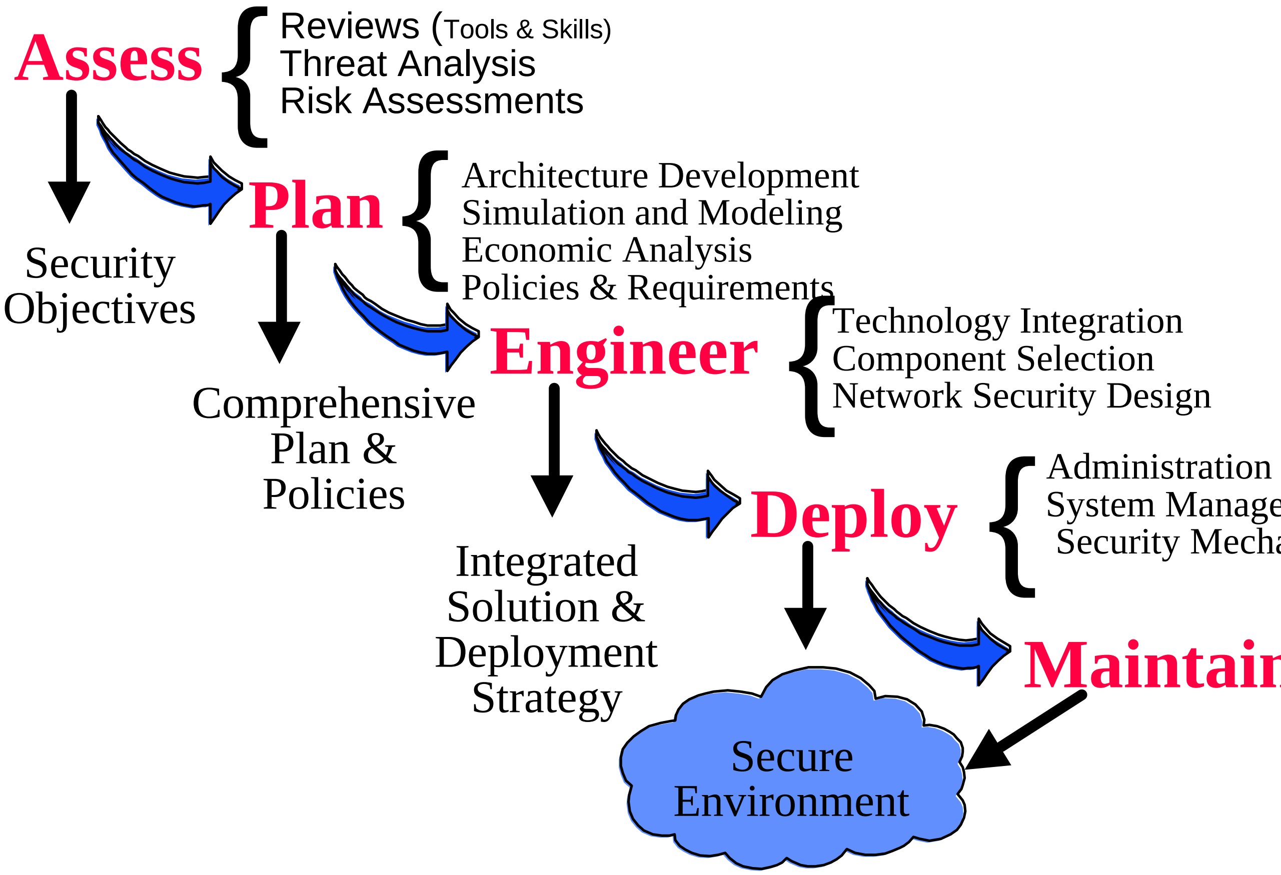
- Firewalls
- End-system security services
- Know where holes are
- Trap & Trace Attempts

Detect Residue

- Intrusion detection – attack signatures
- Forensic Analysis & Trust Mapping
- Detect suspicious/unusual activity

Critical Infrastructure Security
Steps to Success

An Employee-Owned Company



Assess
- Reviews (Tools & Skills)
- Threat Analysis
- Risk Assessments

Security Objectives

Plan
- Architecture Development
- Simulation and Modeling
- Economic Analysis
- Policies & Requirements

Comprehensive Plan & Policies

Engineer
- Technology Integration
- Component Selection
- Network Security Design

Integrated Solution & Deployment Strategy

Deploy
- Administration (Tools)
- System Management & Integrated Security Mechanisms

Maintain
- Monitor (Tools & Skills)
- Security Bulletins
- Incident Response
- Managed Service

Secure Environment

Key Principle: If it isn't in the process, it's unlikely that it will be in the product

A Vision of the Future:
Or a Call to Action?

An Employee-Owned Company

- *"If we can make every American technologically literate, if we can make our government wise not only in its own use of technology but in giving those tools, if we keep building the right kind of information economy which respects privacy and has security, then what we have achieved in the last seven years will be just a small prologue of what will occur in the years ahead."*

  - President Bill Clinton
  Friday, March 3, 2000